

11/18/2007

Online Social Networks and E-Commerce

*Their Threats to Privacy and a Proposal for a New Blanket Privacy Policy
and Accountability Infrastructure for Consumer Online Privacy*

Clarence Lee and Shirley Fung

Table of Contents

Introduction.....	6
Background.....	6
Social Networking and Facebook.....	7
Online Merchants and Amazon.....	8
Joint Services and Advantages for Marketers.....	9
Privacy Protection on Data Collected by Amazon and Facebook.....	10
Data Collected by Facebook	10
Profile.....	10
Social Networks.....	13
News Feeds.....	14
Photos.....	15
Events.....	16
Communications.....	16
Status.....	17
Facebook Applications.....	17
Third-Party Applications.....	19
Automatic Information.....	20
Data Collected by Amazon.....	20
Purchase History.....	21
Wish Lists.....	21
Browsing History and Other Automatic Information.....	21
Affiliates and Third-Party Advertisers.....	22
Problems with Privacy Protection for Online Data and Activities.....	22

[Inconsistencies in the Level of Privacy Protection for Different Kinds of Data.....22](#)

[An Example: Purchase History vs. Browse History.....23](#)

[Current Privacy Policy is Incomplete.....23](#)

.....24

[Summary of Privacy Policy Protections and Exceptions on Data Collected by Facebook and Amazon.....25](#)

[Complexities in Privacy Protection is Confusing to Consumers.....26](#)

[Potential Threats to Privacy.....26](#)

[Scenario 1: Profiling for Anti-Terrorism Investigations.....26](#)

[Scenario 2: Insurance Raising Your Premiums Because of Your Lifestyle.....27](#)

[Proposing a Blanket Privacy Policy Protecting Online Data from Government Intrusion.....28](#)

.....28

[Policy Analysis.....28](#)

[Alternative Policies.....29](#)

[Proposing Privacy Accountability Structure for Third-Party Sites.....30](#)

[Motivation.....30](#)

[The U.S. Approach on Privacy Protection.....31](#)

[The Gramm-Leach-Bliley Act.....32](#)

[Proposed Accountability Structure.....33](#)

[Inform Consumers About Information Stored.....34](#)

[Allow User to Control Data Released.....34](#)

[Require Business to Draft Protection Plan.....35](#)

[Establish Enforcement Authority.....35](#)

[Conclusion.....35](#)

[Appendices.....37](#)

[Amazon.com Privacy Notice.....37](#)

[Facebook.com Privacy Notice.....44](#)

[Bibliography.....53](#)

List of Figures

Figure 1 – Screen shot of a Facebook profile.....	11
Figure 2 – Example of News Feed on Facebook.....	14
Figure 3 – Example of photos section on Facebook.....	15
Figure 4 – Example of the user agreement when adding a third-party application on Facebook.....	18
Figure 5 – Example of gifts displayed on a Facebook profile.....	18
Figure 6 – Example of the Where I’ve Been application displayed on a Facebook profile	20
Figure 7. An exampel of the TRUSTe Web Privacy Seal.....	30

Online Social Networks and E-Commerce

Their Threats to Privacy and a Proposal for a New Blanket Privacy Policy and Standard for Privacy Notices

Introduction

Online service providers, such as Facebook and Amazon, are beginning to collect various kinds of public and private data across the Web for the purposes of targeted marketing. A vast variety of data is collected about the user, and the current legal system has different legal standards for different kinds of data. This is problematic because the privacy policies against government and third-party intrusions are complex and confusing to the end user. To better protect consumers' privacy, all aggregated user data and online activities should be subjected to the same level of protection under a blanket privacy policy. Furthermore, we are proposing an accountability infrastructure for protecting consumer's online privacy.

There are a lot of business marketing incentives to combine the data stored by these online services. Platforms have been introduced by these companies to better combine e-commerce and social networking. Currently, different kinds of data are protected under separate privacy policies and codes. The end user cannot predict how the data can be used by the government or third-parties, or how all their private information would be protected under the existing law.

To limit the scope of the paper, the privacy issues will be focused on the data collected by Amazon and Facebook, and how that data can be shared and used by the government and other third-parties. Even though we are only exploring this hypothetical case study, similar scenarios of companies using data mining and sharing data are already underway. Recently, technology and open APIs (Application Programming Interfaces) has actually been introduced to make large-scale data aggregation on the Web even easier.

Background

Marketers and advertisers are always looking for ways to understand the consumer better. In order to do so, businesses need to gather more information about consumers. Shopping and social networking Web sites gather a lot of information about online users, and has become tremendously useful for companies to

track and model consumer behavior. Businesses are looking to companies like MySpace and Facebook to help companies to sell more products and services.

MySpace has already announced technology that uses profile data to create market segments for advertisers to promote their products to. Application developers are also rushing in to create new widgets for these Web sites. Consequently, users are encouraged to spend more time on the Internet using these services, and companies are getting more incentives to use all the flood of data to improve marketing strategies. There is more personal and sensitive data stored on these online service providers than ever before.

Social Networking and Facebook

Web sites like MySpace, Facebook attract millions of users a year, and people ranging from teens to elders are signing up to use the online social networking services around the world. All these different services have a common theme—the social networks combine people from all around the world who share similar interests and friends. These social networking Web sites provide ways for members to communicate with each other, and give Web space for users to post information about themselves.

These Web sites provide a low cost and convenient way for consumers to stay connected with the members of the Web site. These online social networking platforms also allow user to publish and control content about them easily. The databank of digital information has also helped users better and more quickly find information about others around the world. In 2005, MySpace has exceed Google's page views on the internet, and is expected to continue growing (Rosenbush, 2005). Besides helping users stay in touch with their friends, these Web sites now provide other services like media entertainment, shopping, job search, and many more. These Web sites continue to expand their services to attract more users to sign up, and continue to entice their existing users use the services more.

Facebook started as a social networking Web site for college students, and has opened up for public registration in 2006. The Web site offers basic social networking services such as ways to add other members as your friends. In addition, the Web site allows user to join networks and groups that share the same interest and views. Users can also share unlimited photos with their friends. Facebook also facilitates communications by allowing users to send messages to each other, and post messages on each other's profiles. Friends can also post events and invite guests on Facebook. Facebook also provide a bulletin board for users to sell and buy products from each other.

More interestingly, Facebook has an open platform that software developers can use to create new applications on Facebook. New applications range from horoscopes to ways to arrange an itinerary for a vacation with your friends. Developers range from college coders looking for a fun project to companies looking for ways to take advantage of the mass distribution on Facebook.

There is no stop sign in sight for social networking sites like MySpace and Facebook in the next few years. Users are beginning to be able to do many things virtually on these platforms that they have never imagined before. It is only expected that more kinds of applications would be built to enrich the lives of the online users around the world.

Since social networking sites is still a relatively young phenomenon, most of the information found on Lexus Nexus and Google Scholar are published by major newspapers and magazines. One paper that has been extremely helpful for our research is the 2005 paper titled “Facebook: Threats to Privacy” by Harvey Jones and José Hiram Soltren. In that paper, Jones and Soltren conducted a threat model analysis on Facebook according to Federal Trade commission standards. In addition, they demonstrated potential security loopholes in Facebook with a script, which automatically harvested data from nearly 100,000 students from MIT, Harvard, Oklahoma University, and NYU. Their study found that 92% of all users update their Facebook profile within six months of account creation. In addition, as of 2005, Facebook has reached a base of 8 million users and close to almost 100% penetration at many schools across America. Demographic data and personal interests, the two types of information that advertisers are most interested in, are disclosed by over 70% of the users. Yet despite the fact that all this personal information is stored on Facebook, over 91% and 89% of the respondents had not read the Terms of Service and Privacy Policy, respectively. Without a doubt, the Jones and Soltren paper established two facts: 1) Facebook is ubiquitous and relevant and 2) most users are not informed about privacy.

Because so much sensitive information is being gathered on social networking Web sites, it motivates us to figure out how this new technology would fit within our current privacy legal framework, and to determine the right solution to protect consumer’s privacy on the Internet.

Online Merchants and Amazon

Besides social networking Web sites, many online users visit shopping Web sites to either browse or purchase products. Web sites like Amazon, Yahoo! Shopping or company online stores have revolutionized the retail industry by making it possible for consumers to compare and purchase products from home or office. These online merchants have made it very convenient for a user to buy a book, and have empowered users to browse and compare prices and products. Consumers purchase items such as clothes, electronics, airplane tickets, groceries, etc. Total online sales per year are expected to grow to \$174.5 Billion dollars in the United States (CNNMoney.com, 2007).

As compared to traditional shopping at a mall and stores, the operating costs for an online store can be a lot lower than a storefront type of retailer. In addition, an online shopping site makes it easier for merchants to track online activity. This enables many companies to build large databases of online shopping activities, such as what the consumer has looked at, or what product the user has searched for. These companies now have the data to analyze aggregate and individual consumer behavior. For example,

data such as search query terms and browsing history to better improve the price point and also product selection of the store.

Online advertisers such as DoubleClick have already started using the data to better target advertisement to increase sale of its clients. Amazon.com is one of the first online merchants to improve their advertising strategy by the use of collaborative filtering. Using the purchase history of the customers, Amazon.com shows suggestions for other products by the relation that others who have bought x also bought y.

Amazon started its e-commerce business as an online bookstore, and has grown to be a store that sells items ranging from A to Z (as represented by its logo). Amazon also operates other online stores for retailers such as Target and Marks & Spencer.

Traditionally, consumers have ways to shop without being tracked by visiting the physical store, and pay for their purchases with cash. With these online retailers however, there is no longer an option to shop with privacy. Consumers are required to use a credit card for online transactions, and every click on the Web site (similar to every move you make in a store) is monitored and tracked. This raises some questions about how privacy should be protected in this new setting.

Joint Services and Advantages for Marketers

For marketers, having information from one Web site isn't enough in the increasingly competitive world of e-commerce. Now, companies are interested in knowing what consumers do on Web sites besides their own. For instance, if Amazon knows what the consumer has listed as his/her favorite books and music artists on Facebook, it can better advertise for similar books and CDs on the consumer's next visit to Amazon.com. Another example, if Amazon knows when your birthday is and who your friends are, Amazon can use that information to advertise gifts ideas to your network of friends.

In these scenarios, some consumers find it intrusive that these businesses can know so much about them. Alternatively, when they visit one Web site, should they expect the information to stay within the company, and should never be passed on or sold to another party? There are currently no policies that would protect against these types of situations.

Businesses now value all this information greatly, and are very interested in using it to improve their understanding of individual consumers. In order to make it easier to aggregate data streams, companies have started to provide platforms for integration. Both externally and internally, these companies began to diversify the kinds of services they provide on their Web site using these platforms. In November 2007, Facebook announced a new service called Facebook Beacon. The service allows a user to announce to others in their network about products or services he/she likes. Many online merchants have already signed on as a partner site through Facebook Beacon. Using Facebook Beacon, the users can endorse

products to their friends in the network. These endorsements can help build brand loyalty and reach out to those who are more inclined to listen to recommendations and reviews from their social network.

MySpace has exploited profile data to create micro-segments for companies to focus their marketing communications to, and a similar service is provided by Facebook Ads. Besides advertisements, companies such as Apple or motion pictures such as Pirates of the Caribbean have corporate profile sites and networks on these large social networking sites. These sites help promote for new products or spread the word for promotions. Upcoming motion pictures use these profile sites to provide trailers and local movie times. These company profiles also provide a portal for them to hear reviews directly from their customers.

Google introduced OpenSocial in November 2007 as an attempt to standardize the APIs for many different social networking Web sites. By making it easier for developers to create applications for a large number of social networking Web sites, one can only expect that these cross-site applications will continue to grow in numbers.

Privacy Protection on Data Collected by Amazon and Facebook

Current trends are that these businesses are going to provide more and more services that consumers will participate in. Consumers get the benefits of convenience and fun from these services, and businesses will continue to use this data for commerce purposes. There will be a lot of data mining done on all this data, and consumers need to be aware of the fact that all of this data can be very sensitive information that they may not have adequate privacy protection for.

Data Collected by Facebook

We will now examine the type of information that is possible to be stored on a Facebook profile. In addition, we will also discuss the types of privacy issues that can arise from sharing these types of information. We have attempted to speak with a representative from Facebook, but they had declined to schedule an interview at this time.

Profile

On Facebook, users can voluntarily fill in information about themselves. Facebook profile information is publicly searchable using online search engines, and the user can choose privacy levels on fields in the “contact” portion. The entire Facebook profile also has privacy level settings.

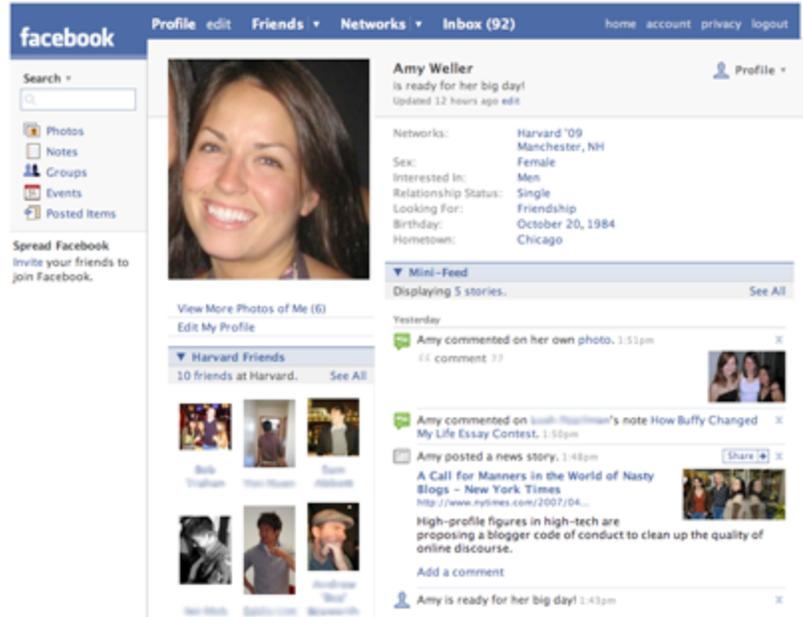


Figure 1 – Screen shot of a Facebook profile

To register for Facebook, a user must provide the following profile information:

- full name (first and last name)
- “in college/graduate school” or “at a company” or “in high school” or none of the above”
 - if the option for school is chosen, educational info for graduation date, status in school is requested
- email address
- date of birth (for age verification purpose)

Upon registration, the user can provide additional personal information about his or herself. The following is a list of fields that a user can fill out (as of November 10, 2007):

- basic
 - sex
 - hometown
 - country
 - political views

- religious views
- contact
 - screen names (instant messengers)
 - mobile phone
 - land phone
 - mailing address (student profiles are specified to room numbers and residences)
 - Web sites
- relationships
 - interested in men and/or women
 - relationship status, and whom you are in a relationship with
 - alternate (maiden) name
 - kinds of relationships you are looking for
- personal
 - activities
 - interests
 - favorite music
 - favorite TV shows
 - favorite movies
 - favorite books
 - favorite quotes
 - about me
- education
 - college/university name

- graduation year
 - degree
- high school name
 - graduation year
- work
 - employer
 - position
 - description
 - city/town
 - time period
- picture
 - profile picture and icon
- other
 - politicians
 - musicians
 - products

Most of these records are not protected by any specific privacy law. Educational records held by a 3rd party are specifically protected by United States Code Title 20 for Education (Center for Democracy & Technology, 2006), requiring that the law enforcement agency must have a subpoena to obtain the information.

Social Networks

Facebook allows users to search for users of Facebook, and to add them as their friends. When adding a friend, Facebook allow the user to add details about the relationship. For instance, a user can add details that the two people have gone to summer camp together, or have traveled together. There are also other networks besides the friends network. Users often join the network of their school based on graduation year, or the network of their workplace.

In addition, users can join groups of other users as well. Example groups include “Join the Breast Cancer Awareness Month”, “Alpha Phi International Fraternity”, “The Official Firefox Community”, and “1,000,000 Strong for Stephen T Colbert”. These groups can be formed around organizations, student groups, common interests, entertainment and arts, or just for fun. Some of these groups can also be sponsored by companies like the clothing retailer American Eagle, and the NBA.

News Feeds

Read Recent News on Your Home Page

When you log in, we'll show you all the latest news and activity from your friends on Facebook in your **News Feed**. Check out photos and notes your friends have added, and see what groups they've joined or created.



Figure 2 – Example of News Feed on Facebook

The News Feeds section aggregates information from users in all of your networks. Any updates within your network would be broadcasted as part of the news feed. These updates include new profile pictures, status updates, or other activities. When this was first introduced, it created a stir among the Facebook members because individuals were concerned that the newsfeed allows others to stalk their friends by the minute. In an article on TIME.com, Tracy Samantha Schmidt wrote, that the “level of intimacy may be too intense for even today's college students” (Schmidt, 2006).

"Every action I take on Facebook is now time stamped," says Erik Ornitz, 18, a Brown student who formed his own anti-News Feed group. "It's a little strange because everyone will now know that at 10 o'clock I updated my Facebook profile and that I wasn't in class." – Erik Ornitz, 18, a Brown student who formed his own anti-News Feed group (Schmidt, 2006)

Photos

Users on Facebook are also allowed to upload photo albums. Levels of privacy protection can be set for these photo albums. Users can label who is in the picture using “tags”. What users may not know is that by uploading a picture, users are also providing embedded metadata on these pictures such as the timestamp and camera make/model used.

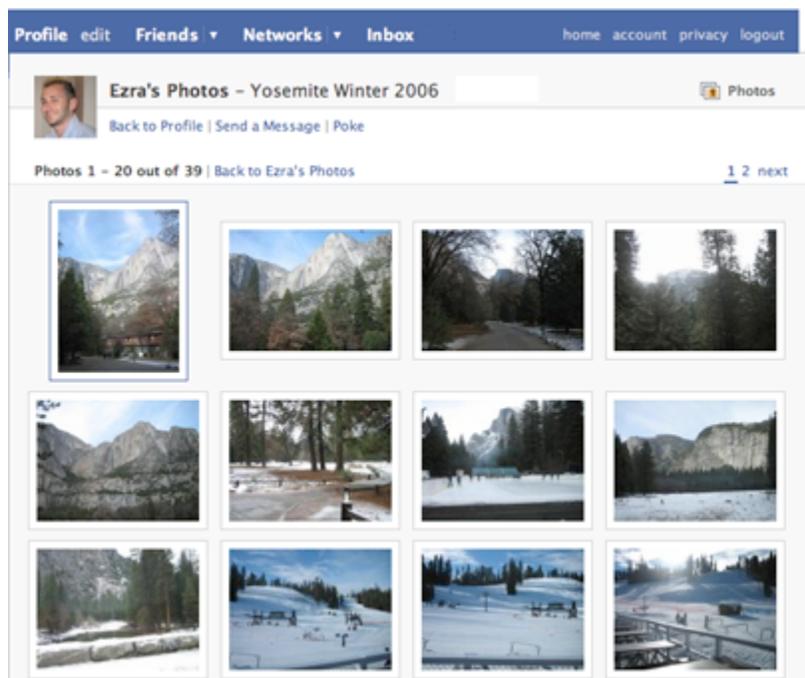


Figure 3 – Example of photos section on Facebook

The alarming thing about the photos feature is that users can only dissociate themselves by removing tags from a photo. However, no current system allows the user to opt out of having their photos posted. If

another user posts an inappropriate picture of you, there is no way for you to remove that picture from Facebook.

Events

Users can host different kinds of events and send invitations for others to come. Many of these events are themed, or held by interest groups. To create an event, the host must provide the following information:

- event info
 - name (required)
 - tagline
 - network (required)
 - host person/group (network)
 - type (required)
- time and place
 - date (required)
 - time (required)
 - location (required)
 - street
 - city/town (required)
- contact info
 - email
 - phone

Facebook provide the functionality to RSVP with a response about the invitee's attendance to keep track of the guest list. Hosts and invitees are allowed to post photos, videos, and messages on the Web space of the event.

There is no specific privacy law that currently covers this kind of information.

Communications

Facebook communications come in many forms. The most rudimentary method of communication comes in the form of Facebook messages that each members can send to each other. Groups can also create mass mailings to send to the members of the group. Event hosts can also send messages to the invitees of the event. These messages are analogous to email. Privacy protection on email communications (less than or equal to 180 days old) are covered under the United States Code Title 18 for Crimes and Criminal Procedure. But emails that are over 180 days old are not protected under current law.

Wall posts, where users can post messages on the profile of another user, group, or event, are a common form of communications on Facebook. However, it is unclear whether this type of public announcement posting is analogous to email. In addition, meta-data such as the time and date that the message was sent, the two parties involved in the transaction as well as the profile picture of the sender are all stored. The Wall-to-Wall feature, a wall communication log between you and another user, also stores the communication history between you that particular party up to the point in which you created your account.

Another major features used on Facebook is the Notes feature. This feature is similar to a Weblog in that the note can be broadcasted to many users at once. Whenever a user writes a note, he can choose whether this note will be broadcasted to other users' newsfeeds.

Status

Facebook users can also post a messages describing what he/she is at a certain moment in time. These statuses are broadcasted to their network of friends. Users are free to say whatever they want in the form: [Name] is [fill in your status here]. Facebook keeps track of these statuses over time.

Facebook Applications

In June 2007, Facebook.com officially launched the Facebook Developers Platform. This opened up Facebook to third-party developers to create applications for on Facebook. A Facebook application is a software solution that can be integrated within the Facebook environment. By allowing commercial and freelance software developers, Facebook has opened up its coveted user communities to various advertisers and businesses.

As of November 15, 2007, there are 8,234 Facebook applications. In addition, the variety of applications types on Facebook is astounding. There are applications ranging from a "Christmas Tree" application that allows you to build a Christmas tree to be put on your profile to the Marketplace that allows you to sell and buy things off Facebook.

Despite all the advantages this influx of applications brings, Facebook applications open up issues of inconsistency in the way user information is stored. Every time a user adds an application, the user is required to grant the application access to your profile information. The problem is that the standard of

privacy protection varies from application to application, and the Facebook Privacy Policy page does not mention a strict standard that all Facebook Applications have to follow.

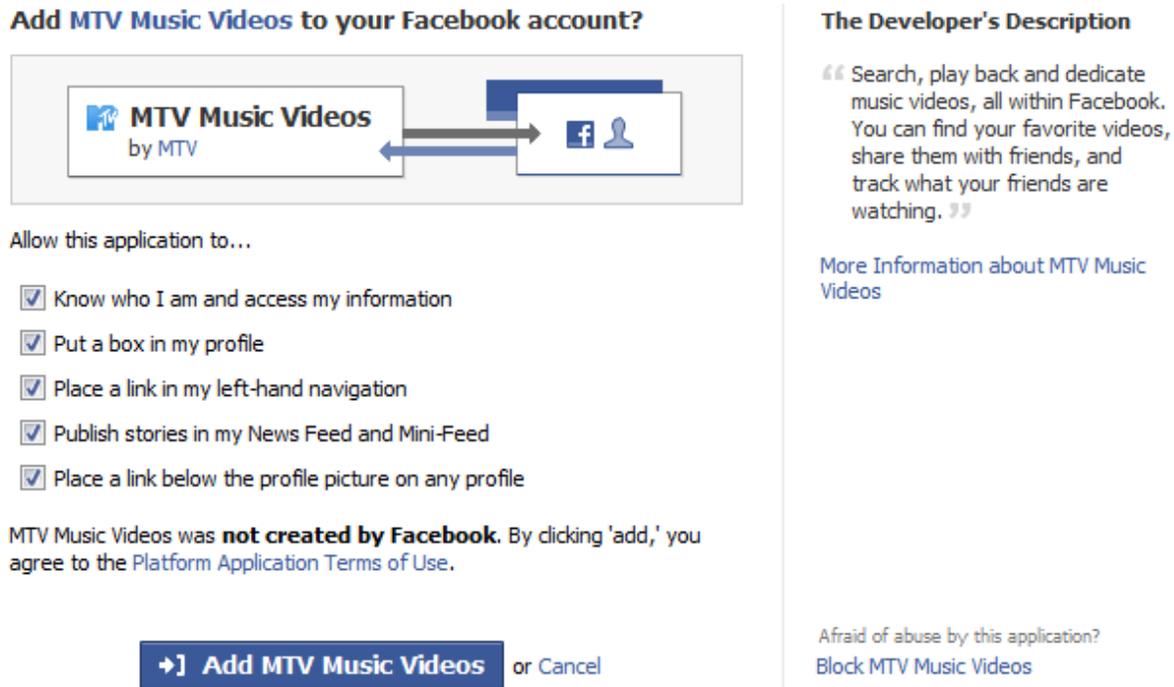


Figure 4 – Example of the user agreement when adding a third-party application on Facebook

Gifts

The Gifts application is a standard application that every Facebook user has. These digital gifts are simply small drawings of items that one user can give to another. Common gift items are flowers, chocolates, and hearts. Every user can send a free gift, and after that, each gift costs USD 1. Once a user receives a gift, the gift icon appears on his profile.

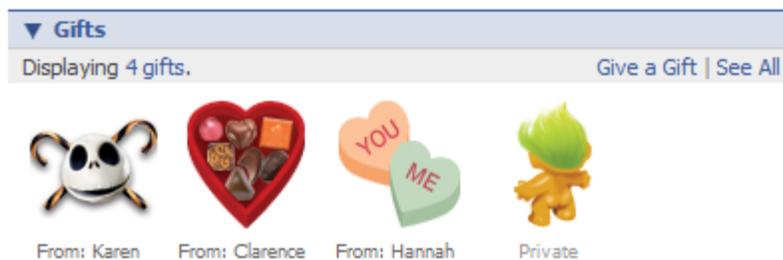


Figure 5 – Example of gifts displayed on a Facebook profile

There are few piece of information that the gift application collects. It stores the sender and receiver names, time of transaction, picture of the gift, private message attached to the gift, and your credit card information for paying the gift.

The only information that the user can opt out of storing is the credit card information, besides that everything else is stored.

Market Place

The Market Place application allows users to buy and sell items on Facebook. This places Facebook in direct competition with sites like Craigslist and eBay. The type of information stored in a market place entry include: user name, date item posted, description of item, number of people viewed, picture, and common friends.

Third-Party Applications

As mentioned before, third-party applications have sprung up by the dozens since the release of the Facebook Developers Standard. We will mention two notable examples of applications that store a rich set of user contents.

SuperWall

The SuperWall application is an enhanced version of the Wall. Aside from allowing users to send messages, SuperWall also allows users to post pictures and videos as well. This application faces the combination of privacy problems faced by the Wall application, pictures, and videos as well.

Where I've Been



Figure 6 – Example of the Where I've Been application displayed on a Facebook profile

The Where I've Been application allows users to specify what areas in the world he has visited, lived, or desires to visit. Aside from storing all of a user's past travel information, the application also stores the user's profile and social network information. From the social network information, it gathers about you, the application allows you to compare your travel map with your friends.

Automatic Information

Aside from the information collected by the various components of Facebook above, there is a certain amount of information that is automatically aggregated whenever you visit a commercial website. Information such as the IP address, browser type, pages visited, time visited, and click stream data are all collected by Facebook. In addition, Facebook explicitly states in their Privacy Policies that your IP address may be sent to third-party advertisers. In addition, companies who advertise with Facebook may download cookies and "web beacons" on to your machine to track the effectiveness of their advertisements. Users should be aware that Facebook states that once the information is out of their hands, they are not held responsible for how third parties use the collected information.

Data Collected by Amazon

Amazon.com collects a lot of information as soon as a user visits the Web site. We requested a short interview with a representative from Amazon.com to understand what procedures are taken to protect consumer privacy against government intrusions. It appears that Amazon.com does consider consumer privacy as an important concern, understanding that book sale records are sensitive personal information. Patty Smith, the Director of Corporate Communications at Amazon.com, stated that "in some cases, [Amazon.com] have challenged the validity of subpoenas when the party seeking the information failed to

demonstrate a compelling need for the information and we believe the request may compromise customer privacy interests.” Even though there is a good amount of privacy protection on sale, we believe that there are other kinds of sensitive data collected by Amazon.com that might not be protected any specific law.

Purchase History

By purchasing, bidding, or auctioning items on Amazon, the history of such actions are stored on Amazon servers. Information stored include the timestamp of purchase, shipping and billing information (i.e. credit card information), and items that you have purchased. These records are covered as sale records with limited privacy protection.

Wish Lists

Customers may also choose to use online wish lists for holiday shopping and wedding registries. These wish lists stores the products that he/she is interested in, and is very informative for figuring out individual consumer behavior and market demand.

Browsing History and Other Automatic Information

The Web site also collects information whenever the user interacts with Amazon.com. As noted in Amazon.com’s Privacy Notice, examples of the automatic information collected on the Web site are (Amazon.com, 2007):

- Internet Protocol (IP) address of the user
- login, email address, password
- browser type, version, browser plug-in types and versions, operating system and platform
- time zone setting,
- full Uniform Resource Locator (URL) click stream to, through, and from Amazon.com
- date and time of the clicks, cookie number
- products viewed or searched for
- cookie data
- session information
 - response times
 - download errors

- length of visits to certain pages
- page interaction information
 - scrolling, clicks, and mouse-overs
 - methods used to browse away from the page

By visiting and using the Amazon.com Web site, users accept the “conditions of use”, which requests users to read the Privacy Notice. If the user never bothered to read either of the documents, they do not know that their user activity is tracked as soon as they visit the site.

Affiliates and Third-Party Advertisers

Amazon.com operates on a business model where the company helps other vendors to sell their products on the Web site. Consequently, your purchasing records are shared with these affiliated in order to fulfill orders. However, the sharing of information is not limited to just purchases; it is foreseeable that Amazon may also pass on consumer behavior information on to these affiliates to increase sales. In addition, companies like DoubleClick work with Amazon to provide different ads for the consumer. Depending on what the user has browsed and purchased, DoubleClick uses cookie data on the browser to determine what advertisements to serve to the user during his/her visit on Amazon.com.

Problems with Privacy Protection for Online Data and Activities

Current policies protecting electronic surveillance only covers email or transactional logs, and seems to be lagging behind the development of all kinds of new activities available on the Internet. After inspecting what the privacy policies are on data collected by Amazon and Facebook, we found numerous problems in the status quo.

Inconsistencies in the Level of Privacy Protection for Different Kinds of Data

Over the past couple decades, more codes and court cases have created a slew of policies and exceptions to different privacy protections on the kinds of data collected by these Web sites. As a result, not all kinds of data are protected under the same privacy policy. Moreover, many different exceptions in the United States Code have put certain types of information at a different level of protection.

For instance, cable TV viewing information is has modest privacy protection under Title 47 of the United States code. In general, government must give the customer or subscriber notice if this information is obtained for an investigation. On the other hand, users can watch online videos from major networks on

Facebook, and that information is stored as internet logs. When these internet logs are used for an ongoing investigation, law enforcement officials do not have to provide notice.

As consumers are spending more and more time on the Web to perform various activities, these internet logs are becoming more meaningful. As a result, investigators can take advantage of these inconsistencies and create loopholes in the system.

An Example: Purchase History vs. Browse History

Amazon.com keeps track of sale records of users' purchases on the online store. Under the Title 18 of the United States Code § 2710(b), a warrant, court order with probable cause, or grand jury subpoena, is needed for real-time interception or immediate seizure.

Amazon.com also keeps track of all the user activity on the Web site. This includes page views to roll over actions on a page. Ways of tracking this type of user activity is by storing the history page requests or image requests. The collection of requests is generally considered as internet logs. According to Title 18 of the United States Code, a high probable cause standard is not needed to obtain internet transactional records (logs) for real-time interception or immediate seizure. Using these logs, such as a list of downloaded images (file requests to the Web server), one can easily deduce what products the user was interested in, and was probably going to purchase.

Contrary to sale records, these internet logs, arguably can provide the same kind of information about the users' purchase habits, are protected under a lower standard than sale records. This is problematic because law enforcement officials can now use data that is protected under a lower standard to construe information that they would have had to get a warrant to obtain. In other words, instead of asking for sale records to paint a picture of a user's buying habits, investigators can simply deduce the purchase habits by asking for the internet logs using a subpoena issued at a lower standard.

In the context of new kinds of online activities on these Web sites, the line between content and non-content communications becomes blurred. Transactional records and use of these online services can generally provide a lot salient information about an individual. Current policies do not protect the rich interactions we currently have on the Web. In addition, data mining has driven companies to create profiles using raw data collected through these Web sites. Even though internet logs are often considered as transactional data, they actually provide a lot more information about the content of the data being downloaded and accessed by users. No policy has been written to protect private information that had been derived from different kinds of data. As a result, we need to have the same standard to protect against abuses of loopholes within the legal system.

Current Privacy Policy is Incomplete

Facebook and Amazon have become leading examples in the industry to provide new kinds of rich interactive application on the Web. For instance, actions that a user can perform on Facebook and other social networking sites have fall outside of what policy makers have accounted for. For instance, there is a long list of private information that is collected by Facebook, that do not fall into any general categories for information collected by third parties. See the following table for the complete list.

Other Records Collected by Facebook, Not Protected Under Any Specific Privacy Policy
PROFILE
political views
religious views
Relationships
interested in men and/or women (sexual orientation)
Activities
Interests
favorites (music, TV shows, movies, books, quotes)
added politicians, musicians, and products
PHOTOS
timestamp of photos taken
camera make/model used
tags of who is in the photo
EVENTS
Location
time and date
Host
guest list
RSVP information of invitees
wall posts
multimedia (photos and videos)
COMMUNICATIONS
wall posts
3RD PARTY APPLICATONS
travel information

Summary of Privacy Policy Protections and Exceptions on Data Collected by Facebook and Amazon

GREEN - STRONG PRIVACY PROTECTION; AMBER - MODEST OR INTERMEDIATE PRIVACY PROTECTION; RED - LITTLE OR NO PRIVACY PROTECTION	Collected by Facebook?	Collected by Amazon?	For real-time interception or immediate seizure, does government need a warrant issued on a HIGH PROBABLE CAUSE STANDARD?	Can government use a subpoena or court order under a LOWER STANDARD?	At time of search/subpoena, must government give the customer/subscriber to whom the information pertains NOTICE?	What are the standards for FOREIGN INTELLIGENCE
Educational Records	YES - School Names and Graduation Dates	NO	NO	YES, 20 USC §§ 1232g(b)(1)(J), 1232g(j)(2), 9007(c)	NO - Prohibited 20 USC § 1232g(b)(1)(J), 1232g(j); 34 CFT 99.31	Court order: relevance standard. Notice prohibited. 20 USC § 1232g(j)
Video Rental & Sale Records	Gray Area - personal interests in movies, TV shows, and music	YES - sale records	warrant, court order with probable cause, or grand jury sub 18 USC § 2710(b)	YES - Plus voluntary disclosure	NO	Court order: relevance standard. Notice prohibited. 50 USC § 1861(A), (D) Plus voluntary disclosure
Other Records Library, Travel and Other Records Not Protected by a Specific Privacy Law	YES - See list of Other Records Collected by Facebook"	YES - Wish lists and Reviews	NO	YES - Plus voluntary disclosure	NO	Court order: relevance standard. Notice prohibited. 50 USC § 1861(A), (D) Plus voluntary disclosure
Email, Unopened, <= 180 Days Old: Unopened email (and voice) in storage for 180 days or less with provider of service to the public	YES - private messages	NO	YES - 18 USC § 2703(a), <i>Exception: Provider can voluntary disclose in emergency, etc 18 USC § 2702</i>	NO	NO - 18 USC § 2703(a)	FISA does not expressly address communications in storage. If stored email is a business record, it is available with a court order upon a showing of reason to believe that it is relevant to a FI/FCI investigation. Notice prohibited. 50 USC § 1861
Email, Opened, <= 180 Days Old: Opened email (and voice) held by provider of service to the public	YES - private messages	NO	IN DISPUTE - 18 USC § 2703, Theofel (9th Cir.), plus emerg, etc	IN DISPUTE - 18 USC § 2703, Theofel (9th Cir.), plus emerg, etc	NO - if warrant; otherwise, can be delayed 18 USC §§ 2703(b), 2705	FISA does not expressly address communications in storage. If stored email is a business record, it is available with a court order upon a showing of reason to believe that it is relevant to a FI/FCI investigation. Notice prohibited. 50 USC § 1861
Email, > 180 Days Old: Opened and unopened email (and voice) in storage for more than 180 days with provider of service to the public	YES - private messages	NO	NO - 18 USC § 2703(a)-(c)	YES - Subpoena or voluntary disclosure in emergency, 18 USC §§ 2702, 2703(c)(2)	NO - if warrant; otherwise, can be delayed 18 USC §§ 2703(b), 2706	FISA does not expressly address communications in storage. If stored email is a business record, it is available with a court order upon a showing of reason to believe that it is relevant to a FI/FCI investigation. Notice prohibited. 50 USC § 1861
Email / Internet Logs (Internet Transactional Records of electronic communications)	YES - click streams, browsing history	YES - click streams, browsing history	NO - 18 USC § 2703(c)(1)	YES - § 2703(d) order or voluntary disclosure in emergency 18 USC §§ 2702,	NO - 18 USC § 2703(c)(3)	NSL: "relevant to" FCI. Notice prohibited. 18 USC § 2709



Source: This chart has been adopted from “Current Legal Standards for Access to Papers, Records, and Communications: What Information Can the Government Get about You, and How Can They Get It?” Version 4.2, July 2006.

Complexities in Privacy Protection is Confusing to Consumers

There are many different legal standards for all the information on Amazon and Facebook, and it is confusing to the user what level of protection each piece of information is entitled to. Not only there is a large collection of information collected by these companies, each kind of private information has different standards of protection depending on the situation. If a user were not a legal expert in the area of internet privacy, he/she would not be able to figure out all the codes and court cases that have shaped the current policies.

Potential Threats to Privacy

Suppose Amazon.com and Facebook.com were to share the data stored by both companies, consumers would face great threats to their privacy beyond privacy issues on one single Web site. The following scenarios are to illustrate how sensitive information about the daily lives of consumers can be revealed from aggregating the data from both sources.

Scenario 1: Profiling for Anti-Terrorism Investigations

You buy a hacker book and you have communicated with people through Facebook (e.g. messages, wall posts, friend requests, and group invitations) from an unfavorable country (e.g. Pakistan, China, Iraq, and Afghanistan ... etc). The Facebook+Amazon entity has created a profile to categorize you of likely middle-eastern decent, and likely a religious fundamentalist. The government could potentially use this profile to link you to terrorists and put you on the “No Fly List”.

In this case, a high-level profile had been created using various kinds of data from Amazon and Facebook. Purchase history and communications are under different levels of privacy protection. It is not clear which privacy policy should the government adhere to. If this type of data mined profiles falls under the “other records” category, then the little or no privacy protection will exist.

Creating this high-level profile from Amazon and Facebook, either one of the parties would have had to pass the personal data to the other party. While these companies generally declare the sharing of data with third parties in their privacy policies, consumers generally do not read, or understand what happens in these policies. In addition, these companies are often not transparent enough to show what happens

behind the curtains. There are currently no policies in the United States that protect the misuse of data being passed on to third parties.

On the other hand, the European Union actually has a directive (95/46/EC) that protects private information by ensuring that a proper procedure has been taken during the action of passing data onto another party. As of now, there is no such standard to protect consumer privacy in the United States. Many transnational companies have adopted the policy to ensure that they meet the guidelines in the European Union, but it is unclear whether domestic U.S. companies will follow suit.

Non-profit organizations, such as TRUSTe, have begun to allow online businesses to be certified as a TRUSTe member. TRUSTe gives out different seals for businesses for different kinds of standards. One of them is the Web privacy standard. To obtain the seal for Web privacy, businesses are required to have an approved privacy notice, disclosure of practices, and provide mechanisms for choice and consent.

Without enough pressure from the public, online businesses will not have an incentive to meet these guidelines. Moreover, this action is completely voluntary, and has no infrastructure for accountability when something does go wrong. Without accountability and legal binding, this system will not adequately protect consumer privacy. For instance, even though TRUSTe requires disclosure of how sensitive data is used, it does not guarantee that misuse of customer's sensitive data would have any adverse consequences on the businesses.

Scenario 2: Insurance Raising Your Premiums Because of Your Lifestyle

You have browsed and searched for books on skydiving, and have posted on your public Facebook profile that you enjoy extreme sports. For the purposes of better marketing, Amazon and Facebook as used this data to label you as the "extreme adventurer," so that they can send you regular email newsletters about mountain climbing, white water rafting, etc. Your health insurance company purchases this information from Amazon and Facebook, and has decided to raise your health insurance premiums this year.

As browsing history and purchase history become more and more informative, companies can deduce all kinds of characteristics about consumer behavior. While companies can use the information to better promote products that suits your needs, there are times where this information can be held against you, as illustrated in scenario 2. For instance, if you have posted pictures on Facebook of your sports car, and joined a forum for underground street racing enthusiasts, car insurance can raise your premiums. Likewise, your browsing and search history of WebMD.com may help health and life insurance companies to determine what your health risks might be.

Most often, consumers would use a Web site and never think that this information can be held against them in another context. While companies may disclose this information to another party, consumers rarely know what exactly had been disclosed, and how the information was used. In addition, when harm

was done, like in this scenario, consumers may not even know why their insurance premiums were increased.

Proposing a Blanket Privacy Policy Protecting Online Data from Government Intrusion

As described in the previous sections, there are several issues with the status quo. The proposal to have a blanket privacy policy is to prevent further government intrusions on privacy over online data and communications. In addition, a simpler policy will be easier for citizens to understand. All online data and communications should be treated equally under this new policy.

Policy Analysis

A blanket policy will aim to ensure that all online communications and data stored by third parties to be protected under a high level of protection against the government. In order for the government to obtain information such as all email or internet logs, a warrant issued on a high probable cause needs to be required. In doing so, government officials need to meet a higher standard of proof for how this information is relevant to the current investigation.

It is clear that there is an intrusion of privacy when the government would like to get their hands on data on these Web sites, but it is unclear why different kinds of data are protected under different levels of protection. It is illustrated in this paper that the electronic communications stored on various online services providers are all information that can reveal a lot of sensitive information about individuals.

As more kinds of activities arose on the Internet, policy makers and court rulings have been creating patchwork to determine what kind of data should be covered under which kind of privacy protection. What they have failed to realize is that all the different kinds of information can provide a lot of information about an individual. Consequently, data protected under a lower standard, became loopholes in our legal system for electronic surveillance. This opens up areas where investigators can deduce similar information using information such as internet logs, which can be easily obtained with a court order.

Having a blanket policy protection will protect all online activities as a whole, so that it would provide a more comprehensive protection on our privacy. It would effectively remove artificial exceptions such as whether an email was opened or unopened, or whether the email was 180 days old or not. Such a policy would be easier to understand and enforce. As technology evolves, we may expect that other kinds of data would be used and stored by third parties. A blanket policy would be advantageous because it would continue to cover new kinds of online records.

Critics may argue that the reason why there are many different standards is that not all information has the same level of sensitivity, and should not deserve the same kind of protection. However, as data become more connected through data mining and other kinds of data analyses, it would become difficult to determine which provision is applicable. In the digital age, passing and connecting of data is a lot easier than the age of paper records. No longer protected by practical obscurity, sensitive digital information can flow to other kinds of information very quickly. It is often hard to separate things such as an individual's internet logs and library records.

Alternative Policies

Recordable online activity with the influx of personal data in social networking Web sites has changed the way that we should view privacy on the Internet. Some may argue that online activities should not be protected at all, because society no longer has an expectation of privacy on the Internet whatsoever. Nevertheless, it is hard to believe that society is ready to abandon all expectation of privacy just because any activity is logged on the Internet. Perhaps we can no longer use the same metaphors to describe how different kinds of digital information are protected. It is important to reconsider what online activities are in the views of the Fourth Amendment.

In the judicial opinion of the U.S. Supreme Court case *Katz vs. United States*, it is clear that electronic surveillance of data stored by a third party is still considered a legitimate intrusion because "the Fourth Amendment protects people, not places" (*Katz vs. United States*, 1967). If this is so, it becomes a question of whether consumers have a reasonable expectation of privacy with their online data and activity. In a small survey conducted at the Massachusetts Institute of Technology, all respondents, eight students and staff members expressed discomfort of the government being able to obtain information stored by Amazon and Facebook.

Students agreed that if the information is public, the government has fair game to use that information against the individual. However, for the information that is regarded as private, respondents were agreed that the government should not be able to get the information easily. One of the respondents said that government intrusion on your Facebook data "is like eavesdropping on communications, friends talking with friends. The government is not really your friend." The respondent added, "This is like wiretapping, they need probable cause, it's the same thing as email and phone records. If they can show that, then I would be okay with it." In regards to purchase and browse history on Amazon, the respondent also had an expectation of privacy, and said that he "wouldn't want [Amazon] to publish what I bought or browsed to everyone on the Web."

Perhaps our online activity is merely an extension of what we do in our own homes, and we should be given the right to be left alone. Just because we now have the luxury to chat with someone across the globe, this does not mean that we ought to give up the right to privacy that we have as if we were just talking to our friends at home.

Proposing Privacy Accountability Structure for Third-Party Sites

Motivation

In addition to the blanket privacy policy to protect the consumer's rights from the government, we propose to a privacy accountability structure to hold third party sites accountable. During the 1990's, phishing attempts on America Online drew much public attention to Internet security and privacy protection. It is estimated that businesses loses two billion USD each year as their clients become victims of identify theft (Kerstein, 2005). Since then, Internet security and privacy protection has gotten much better. Non-profit organizations such as TRUSTe and Better Business Bureau Online have been founded to serve as watchdogs to verify the integrity of Third-Party websites. However, we should not stop there.

One of the biggest criticisms of organizations such as TRUSTe is that they do not have much power to punish violators. While it is commended for its attempts to establish trust between businesses and consumers, TRUSTe does not do enough to punish its seal holders who break their Web Privacy Seal agreements, and it does not revoke their seals quick enough.



Figure 7. An example of the TRUSTe Web Privacy Seal.

In August, 2006, America Online accidentally release three months worth of search queries by more than 600,000 AOL users (AOL Heads Roll Over Data Leak, 2006). Despite the fact that usernames were not released, a New York Times article demonstrated that one could identify an individual's name and residing city given enough search queries (Barbaro & Zeller, 2006). In response, AOL fired three employees, including its chief technology officer, and issued a public apology.

Only one month later, the online social networking program SecondLife suffered a security breach, releasing vital information for 650,000 customers (LeClaire, 2006). SecondLife is a highly successful Massive Multiplayer Online Role Playing Game (MMORPG). It allows users to start a "second life" in a massive virtual world, complete with land ownership, jobs, and a fully working economy. Users can purchase goods using the LindenDollar, the currency within the virtual world, and exchange services just as one would in real life. From the incident, vital information such as unencrypted user name, addresses, encrypted passwords, and encrypted billing information were compromised. However, despite such a blunder, the only thing that SecondLife did was inform its users of the breach and recommend users to reset user password immediately. SecondLife currently boasts more than 10 million users world-wide, and

an estimate of over one million USD was spent within the SecondLife economy over the past twenty four hours (Second Life Economics Statistics Page, 2007).

Given the massive amount of information aggregated at each of these sites, it raises two important questions: 1) whether all this data should be centralized in one service, and 2) whether the current privacy protection standards are sufficient to safeguard the interest of consumers.

The first question poses interesting legislative possibilities to prevent the monopolization of information. However, on the downside, this would inhibit innovation on the business side and convenience on the end-user side. For the scope of this paper, this issue will not be discussed, since an accountability structure applies whether an information monopoly exists or not.

The second question points the user to seek what is currently available to protect the user privacy. As mentioned before, currently the best systems for privacy protection available are non-profit watchdog organizations such as TRUSTe to look out for the best interest of consumers. However, the biggest problem with this system is the lack of accountability. It is easy to see that in a brick-and-mortar analogy, sensitive user personal information such as billing information and medical history would be guarded with the utmost care. Storage facilities would employ guards, install safes, and use other security measure to prevent theft of such valuable information. In addition, standards and law are in place to hold organizations accountable to safeguard this information. Considering that online information can be copied with more ease than tangible physical documents, and digital storage makes it possible to aggregate information ten to hundreds of orders of magnitude than a physical storage house, shouldn't we have a better accountability measure to ensure the protection of digital information?

Hence, for this proposal, we will first compare the privacy philosophy of the United States versus that of the European Union and the advantages of the European Union Directive on Data Protection. Then, we will propose similar guidelines based on the privacy regulation with the financial industry brought on by the Gramm-Leach-Bliley Act.

The U.S. Approach on Privacy Protection

The United States currently takes a sectorized approach to data protection and privacy legislation. Instead of using an over-arching governmental structure like the EU Directive, it relies on a combination of legislation, regulation, and self-regulation to protect user data. In 1997 report titled "A Framework for Global Electronic Commerce, former President Bill Clinton and former Vice President Al Gore stated that the private sector should lead the efforts in self-regulation in order to protect the consumer from problems brought by the advancement of Internet technology (Clinton & Gore, 1997). As a result, United States does not have a comparable privacy law such as the EU Directive, and privacy law in the United States are adopted on an as-need basis.

It has been nearly ten years since the release of that report, and the Internet has dramatically changed since then. Given the increased level of comfort that consumers feel with online shopping as well as the current Web 2.0 boom of social networking sites, personal data stored on the Internet has grown exponentially. From the cases aforementioned, it is clear that some action needs to be taken in order to safeguard consumer data.

While drafting an over-arching government legislature would be the best option in protecting consumer privacy, it would be unfeasible given the current United States economic and political environment. In addition, doing so would violate the American laissez-faire economic philosophy that has guided the American economy for many years. What we are proposing is to follow the current adoption-as-needed approach and to create an accountability structure specific to the electronic commerce industry. Given that the information stored on sites such as Facebook and Amazon are similar to the financial and personal information stored by banks and insurance agencies, we will discuss the history and policy implications of the Gramm-Leach-Bliley Act.

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was passed in 1999 as an effort to modernize the financial industry. After the Great Depression, Congress passed the Glass-Steagall Act to prohibit the merger between national and state banks with security companies. In 1956 and 1982, Congress passed and amended the Bank Holding Company Act that forbids a bank from controlling a non-bank company and prevented insurance agencies from merging with banks. Then, in 1999, GLBA allowed banks to engage in some of these previous activities (The Gramm-Leach-Bliley Act, 2005).

One of the main reasons why banks and insurance companies were prevented from merging before is the fear of a merged company holding too much information about its clients. After GLBA, the banks that hold one's financial information can merge with insurance companies that hold one's medical record. This allowed the merged companies to sell consumer information to third parties that resulted in several prominent lawsuits that brought this problem to public attention.

In 1997, Charter Pacific Bank of California sold customer information and credit card numbers to an adult Web site company. In turn, the adult Web site billed over 900,000 consumers for a total of 42 million USD for adult content access (\$37.5 Million Judgment Against Porn Site, 2000).

A year later, Nations Bank sold customer information to its subsidiary Nations Securities. Nations Securities in turn convinced many low-risk customers to invest in high-risk investments. Many low-risk customers, a majority were senior citizens, lost significant amounts of their life savings.

From these examples, it is clear that self-regulation do not work when the interest of the business conflicts with protecting customer data. In the case of many social networking sites, where the main source of

revenue is from advertisers, it also seems to be a conflict of interest to depend on these companies to self-regulate privacy protection.

In addition, the European Union expressed privacy protection concerns over European banks conducting business with American banks. Furthermore, the EU was especially worried about the American preference for self-regulation. Privacy laws were more developed in Europe and the EU passed the Data Protection Directive in 1995 to serve as an overarching legislature that enforced privacy protection in all EU nations. Even though the United States Government drafted the Safe Harbor proposal with the EU, this was not enough to protect consumers. One should also note that under the Safe Harbor principles, the Federal Trade Commission has not challenged any companies for failing to meet program standards yet. To bring this back to the electronic commerce industry, it is questionable how effective current privacy enforcement is, especially when the banking industry, storing similar information, required Congress to pass the GLBA provisions to protect consumers.

This caused Congress to include Title V in the GLBA provisions. Title V include three parts:

1. **Financial Privacy Rule.** This rule requires all financial institutions to release privacy notice to the consumer at the beginning of their business relationship and annually thereafter. The financial institution must also report what kind of information is collected about the user, where that information is shared, and how that information will be used. According to the Fair Credit Reporting Act, the notice must also inform the user of his option to opt-out of having their information shared with an unaffiliated third party.
2. **Safeguard Rule.** This rule mandates that business should develop a written, formal, information security plan to safeguard customer data. The plan must include the following elements:
 - a. Assigning at least one employee to manage the safeguard measures.
 - b. Constructing a risk management on all departments that handles the information requiring protection.
 - c. Developing and testing a program that can secure the customer information
 - d. Outlining steps to change this plan as needed.
3. **Pretexting Rule.** This is the rule that provides privacy protection against social engineering. Financial companies must take measures to defend customer information against forms of social engineering attacks such as phishing and pretexting. Note that pretexting is illegal under U.S. law.

Proposed Accountability Structure

Similar to Title V of GLBA, our proposed accountability structure should serve four purposes: 1) inform consumer about the types of information stored, 2) allow user to have control over what data to be released, 3) standardize and require all businesses to draft protection plan, and 4) establish enforcement authority.

Inform Consumers About Information Stored

While the Financial Privacy Rule holds business accountable to educate the user about privacy protection, one of the biggest complaints is that there is no standardized way of displaying that information to the user. GLBA leaves the burden of deciding the format in which the privacy policy is present on the business, and hence many businesses would often present the privacy policy in a long and convoluted manner in order to discourage the consumers from reading it. This defeats the purpose and we propose that an easy to understand structure to be established to educate the user.

One possibility would be to leverage the Platform for Privacy Preferences (P3P) Project. Developed by the World Wide Web Consortium, the P3P Project “enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents (Platform for Privacy Preferences (P3P) Project).”

Another possibility would be to use a simple visual chart to display the kinds of information stored on third party Web sites. Similar to the Nutritional Facts chart found on all packaged foods in the United States, a simple, standardized chart like that can effectively educate the user about information stored.

Allow User to Control Data Released

Another improvement upon the GLBA system would be to provide a simple way for users to opt-out. While the current GLBA system allow users to opt-out from having their Financial information shared with non-affiliated companies, the opt-out description is often confusing to read and hard to understand. This places the burden of decision on the consumer to learn about the possible opt-out options and actually going through the complicated procedures of opting-out. While this sounds like it is trying to protect the consumer on paper, in reality the rule is not very effective. Companies can do whatever they want with the consumer data as long as the user does not opt-out, hence this creates an incentive for businesses to make the opt-out procedure to be as complicated as it can be.

Having an easy-to-understand opt-out description would actually give consumers the power of decision. While we could have proposed an opt-in system where users have to opt-in to allow companies to share any consumer information at all, we feel that this would be too restricting on businesses in that almost no consumer would actually volunteer to have their information be shared. Since we believe that this option will garner much resistance from businesses, we feel that the clear opt-out approach would be a better compromise.

Require Business to Draft Protection Plan

We propose that a similar plan to the Safeguard Rule to be applied to third party Web sites. This establishes a standard requiring all Web sites having to store user information to comply. In addition, the major benefit of an established system such as this is to help consumers understand the steps taken to protect their data.

Establish Enforcement Authority

Lastly, the most important part of our proposal is to establish enforcement authority. While enacting GLBA enforcement structure for our proposal would be a big step forward for protecting online customer privacy, we feel that there is a way that the enforcement authority could be enhanced.

The biggest problem with the GLBA enforcement structure is that it places the burden of enforcement entirely on the Federal Government. We recommend that the state government to have to power of enforcement as well. While one may contest this notion by pointing out the fact that a particular Web site may store user data from all 50 states, such ambiguity could be enforced by the state in which the Web site's creators reside in. Similar to how the United States Court Circuit alleviate burden off the Supreme Court, this method will alleviate the Federal Government's burden of enforcing this accountability structure in all fifty states.

Conclusion

Unlike ten years ago, the Internet has grown to be a common household commodity. Social networking sites and e-commerce sites has enjoyed a period of immense growth. As the popularity of these Web sites increase, the gap between our virtual life on the Internet and our real life in the physical world becomes smaller and smaller. As a result, we must reexamine whether the privacy policies implemented years ago should be updated in order to keep up with the incredible progress of technology.

For this paper, we examined two types of Web sites: e-commerce Web sites and social network Web sites. The combination of both makes up a significant portion of Web traffic. In addition, we looked at two specific examples: Amazon and Facebook, and we examined the types of user information that is stored on both.

Due to the massive amount of personal data stored on both of these Web sites, we proposed two solutions to ensure consumer privacy protection. The first is to require a blanket protection policy to protect private data from government intrusion. Given that the type of data on these Web sites can tell someone a lot of a user, a blanket protection policy is needed to protect all data so one cannot circumvent the system by acquiring information in a less protected category.

The second solution is to propose a standardized accountability structure for protecting privacy data from third-party intrusion. This proposal is inspired by Title V of the Gramm-Leach-Bliley Act, and it standardized the way all financial institutions deal with customer privacy.

Ultimately, it is important to often re-examine our assumptions about our policies every once a while to make sure that the policies are not brought outdated by the latest technology. We suggest that the recommendations made in this paper must be regarded with respect to the technology available in our time, and these same assumptions must be checked in the future to ensure the privacy protection of our fellow citizens.

Appendices

Amazon.com Privacy Notice

Amazon.com Privacy Notice

Last updated: August 29, 2007. To see what has changed, [click here](#).

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

- [What Personal Information About Customers Does Amazon.com Gather?](#)
- [What About Cookies?](#)
- [Does Amazon.com Share the Information It Receives?](#)
- [How Secure Is Information About Me?](#)
- [What About Third-Party Advertisers and Links to Other Websites?](#)
- [Which Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon.com?](#)
- [Does Amazon.com Participate in the Safe Harbor Program?](#)
- [Conditions of Use, Notices, and Revisions](#)
- [Examples of Information Collected](#)

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

- **Information You Give Us:** We receive and store any information you enter on our Web site or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com. [Click here](#) to see examples of the information we receive.
- **E-mail Communications:** To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers. If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#).

- **Information from Other Sources:** We might receive information about you from other sources and add it to our account information. [Click here](#) to see examples of the information we receive.

What About Cookies?

- Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your Web browser to enable our systems to recognize your browser and to provide features such as [1-Click](#) purchasing, [New for You](#), personalized [Amazon Honor System](#) greetings, and storage of items in your Shopping Cart between visits.
- The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Website of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

Does Amazon.com Share the Information It Receives?

Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

- **Affiliated Businesses We Do Not Control:** We work closely with our affiliated businesses. In some cases, such as Marketplace and Auctions sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. [Click here](#) for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions, and we share customer information related to those transactions with that third party.
- **Third-Party Service Providers:** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.
- **Promotional Offers:** Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your [Customer Communication Preferences](#).
- **Business Transfers:** As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.
- **Protection of Amazon.com and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our [Conditions of Use](#) and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud

protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

- **With Your Consent:** Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?

- We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.
- We reveal only the last five digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
- It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

What About Third-Party Advertisers and Links to Other Websites?

Our site includes third-party advertising and links to other websites. We do not provide any personally identifiable customer information to these advertisers or third-party websites. [Click here](#) for some examples as well as information on how to contact these companies to learn more or opt-out of their information collection practices.

These third-party websites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our website directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize advertising content. We do not have access to or control over cookies or other features that they may use, and the information practices of these advertisers and third-party websites are not covered by this Privacy Notice. Please contact them directly for more information about their privacy practices. In addition, the [Network Advertising Initiative](#) offers useful information about Internet advertising companies (also called "ad networks" or "network advertisers"), including information about how to opt-out of their information collection.

Amazon.com also displays targeted advertising based on personal information about users. Although Amazon.com does not provide any personal information to advertisers, advertisers (including ad-serving companies) may assume that users who interact with or click on a targeted advertisement meet the targeting criteria used to display the ad (for example, users in the northwestern United States who like classical music).

Which Information Can I Access?

Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating

that information. [Click here](#) to see some examples, the list of which will change as our Web site evolves.

What Choices Do I Have?

- As discussed above, you can always choose not to provide information, even though it might be needed to make a purchase or to take advantage of such Amazon.com features as [your Profile](#), [Wish Lists](#), [Customer Reviews](#), and [Amazon Prime](#).
- You can add or update certain information on pages such as those listed in the "[Which Information Can I Access?](#)" section above. When you update information, we usually keep a copy of the prior version for our records.
- If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#). (If you do not want to receive [Conditions of Use](#) and other legal notices from us, such as this Privacy Notice, those notices will still govern your use of Amazon.com, and it is your responsibility to review them for changes.)
- The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Website of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

Are Children Allowed to Use Amazon.com?

Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian.

Does Amazon.com Participate in the Safe Harbor Program?

Amazon.com is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the [U.S. Department of Commerce's Safe Harbor](#) Web site. If you would like to contact Amazon.com directly about the Safe Harbor program, please send an e-mail to safeharbor@amazon.com.

Conditions of Use, Notices, and Revisions

If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our [Conditions of Use](#), including limitations on damages, arbitration of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon.com, please [contact us](#) with a thorough description, and we will try to resolve it.

Our business changes constantly, and our Privacy Notice and the [Conditions of Use](#) will change also. We may e-mail periodic reminders of our notices and conditions, unless you have instructed us not to, but you should check our Web site frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information

- [Conditions of Use](#)
- [Web-based Discussion Service](#)
- [Amazon.com Marketplace and Auctions Participation Agreement](#)
- [Marketplace and Auctions Account and Community Guide](#)
- [Help department](#)
- [Recent Purchases](#)
- [Your Profile Guidelines](#)

Examples of Information Collected

Information You Give Us

You provide most such information when you search, buy, bid, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com or one of our third-party sellers; make an Auction bid or purchase; provide information in [Your Account](#) (and you might have more than one if you have used more than one e-mail address when shopping with us) or [Your Profile](#); communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; compile [Wish Lists](#) or other gift registries; provide employer information when opening a corporate account; participate in [Discussion Boards](#) or other community features; provide and rate [Reviews](#); specify a [Special Occasion Reminder](#); share information with [Amazon Friends](#); and employ other Personal Notification Services, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in [1-Click](#) settings; e-mail addresses of [Amazon Friends](#) and other people; content of reviews and e-mails to us; personal description and photograph in [Your Profile](#); and financial information, including Social Security and driver's license numbers.

Automatic Information

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and timezone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as [Purchase](#).

[Circles](#) and [Top Sellers](#); the full Uniform Resource Locator (URL) click stream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; your Auction history; and the phone number you used to call our 800 number. We may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects), or similar data on certain parts of our Website for fraud prevention and other purposes. During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

Information from Other Sources

Examples of information we receive from other sources include updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily; account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services (such as Target.com, BombayCompany.com, and DVF.com); search term and search result information from some searches conducted through the Web search features offered by our subsidiaries, Alexa Internet and A9.com; search results and links, including paid listings (such as Sponsored Links); and credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

Third-Party Advertisers and Links to Other Websites

Examples of third-party advertisers and advertising companies that you can link to from the Amazon.com website or that serve advertising content directly to your browser on certain Amazon.com pages include [Doubleclick](#). You can find out more about its information collection and use practices, including how to opt out of cookies and other collection techniques that it uses, by clicking on the above link to its website.

Information You Can Access

Examples of information you can access easily at Amazon.com include up-to-date information regarding recent orders; personally identifiable information (including name, e-mail, password, communications preferences, address book, and 1-Click settings); payment settings (including credit card information and gift certificate, gift card, and check balances); e-mail notification settings (including Alerts, Available to Order notifications, Delivers, New for You, Special Occasion Reminders, Weekly Movie Showtimes, and newsletters); recommendations (including recent product view history, prior order history, and Favorites); shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries); Auctions and Marketplace seller accounts; and your Profile (including your product Reviews, Requests, and Recommendations, Listmania lists, "So You'd Like to..." guides, personal profile, people you tagged as interesting, and Amazon Friends).

Co-branded and Joint Offerings

Examples of businesses with which we offer joint or co-branded products and other offerings include Target, Borders, Waldenbooks, CD Now, Verizon Wireless, Sprint, T-Mobile, Cingular, Shutterfly, Office Depot, J&R, PetSmart, Godiva, FTD, Avon, Bombay Company, Macy's, PacSun, Eddie Bauer and Northern Tool + Equipment.

Facebook.com Privacy Notice

This policy is effective as of September 12, 2007.

Facebook Principles

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information.

Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the [My Privacy](#) page.

2. You should have access to the information others want to share.

There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com.

Safe Use of Facebook

For information for users and parents about staying safe on Facebook, [click here](#).

Facebook's Privacy Policy



Facebook's Privacy Policy is designed to help you understand how we collect and use the personal information you decide to share, and help you make informed decisions when using Facebook, located at www.facebook.com and its directly associated domains (collectively, "Facebook" or "Website").

By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.

Facebook is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. This privacy statement covers the site www.facebook.com and its directly associated domains. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe.

If you have questions or concerns regarding this statement, you should first contact our privacy staff at privacy@facebook.com. If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should contact TRUSTe Watchdog at http://www.truste.org/consumers/watchdog_complaint.php. TRUSTe will then serve as a liaison with us to resolve your concerns.

EU Safe Harbor Participation

We participate in the EU Safe Harbor Privacy Framework as set forth by the United States Department of Commerce. As part of our participation in the safe harbor, we have agreed to TRUSTe dispute resolution for disputes relating to our compliance with the Safe Harbor Privacy Framework. If you have any complaints regarding our compliance with the Safe Harbor you should first contact us at info@facebook.com. If contacting us does not resolve your complaint, you may raise your complaint with TRUSTe at http://www.truste.org/users/users_watchdog_intro.html.

The Information We Collect

When you visit Facebook you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site.

When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us.

When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A

cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature.

When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information.

You post User Content (as defined in the Facebook [Terms of Use](#)) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is a violation of the Facebook Terms of Service and should be reported to privacy@facebook.com.

If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will automatically send your friend a one-time email or instant message inviting him or her to visit the site. Facebook stores this information to send this one-time invitation, to register a friend connection if your invitation is accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database.

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at info@facebook.com.

Children Between the Ages of 13 and 18

We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook

When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email address to send you notifications regarding new services offered by Facebook that we think you may find valuable.

Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network and those limited pieces of information may be made available to third party search engines. This is primarily so your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

Facebook may send you service-related announcements from time to time through the general operation of the service. For instance, if a friend sends you a new message or poke, or someone posts on your wall, you may receive an email alerting you to that fact.

Generally, you may opt out of such emails [here](#), though Facebook reserves the right to send you notices about your account even if you opt out of all voluntary email notifications.

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links).

Sharing Your Information with Third Parties

Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you. For example:

Your news feed and mini-feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your news feed and mini-feed [here](#).

Unlike most sites on the Web, Facebook limits access to site information by third party search engine "crawlers" (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g. number of wall postings).

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.

If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the [Privacy Settings](#) page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data. Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review these terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action.

We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to

comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.

We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.

We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.

If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this information may become publicly available.

Links

Facebook may contain links to other websites. We are of course not responsible for the privacy practices of other web sites. We encourage our users to be aware when they leave our site to read the privacy statements of each and every web site that collects personally identifiable information. This Privacy Policy applies solely to information collected by Facebook.

Third Party Advertising

Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about where individuals using your

computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them.

This privacy policy covers the use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers.

Changing or Removing Information

Access and control over most personal information on Facebook is readily available through the profile editing tools. Facebook users may modify or delete any of their profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the [My Account](#) page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., sending a personal message to another Facebook user) you generally cannot remove such communications.

Security

Facebook takes appropriate precautions to protect our users' information. Your account information is located on a secured server behind a firewall. When you enter sensitive information (such as credit card number or your password), we encrypt that information using secure socket layer technology (SSL). (To learn more about SSL, go to http://en.wikipedia.org/wiki/Secure_Sockets_Layer). Because email and instant messaging are not recognized as secure communications, we request that you not send private information to us by email or instant messaging services. If you have any questions about the security of Facebook Web Site, please contact us at privacy@facebook.com.

Terms of Use, Notices and Revisions

Your use of Facebook, and any disputes arising from it, is subject to this Privacy Policy as well as our Terms of Use and all of its dispute resolution provisions including arbitration, limitation on damages and choice of law. We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's new effective date. If we make material changes to this policy, we will notify

you here, by email, or through notice on our home page. We encourage you to refer to this policy on an ongoing basis so that you understand our current privacy policy. Unless stated otherwise, our current privacy policy applies to all information that we have about you and your account.

Contacting the Web Site

If you have any questions about this privacy policy, please contact us at privacy@facebook.com. You may also contact us by mail at 156 University Avenue, Palo Alto, CA 94301.

Bibliography

\$37.5 Million Judgment Against Porn Site. (2000, September 8). Retrieved November 18, 2007, from ConsumerAffairs.com: http://www.consumeraffairs.com/news/x_scam.html

Amazon.com. (2007, August 29). *Privacy Notice*. Retrieved November 10, 2007, from Amazon.com: <http://amazon.com/gp/help/customer/display.html/102-7947306-0882551?ie=UTF8&nodeId=468496>

AOL Heads Roll Over Data Leak. (2006, August 22). Retrieved 11 18, 2007, from ConsumerAffairs.com: http://www.consumeraffairs.com/news04/2006/08/aol_firings.html

Barbaro, M., & Zeller, J. T. (2006, August 9). *A Face Is Exposed for AOL Searcher No. 4417749*. Retrieved November 18, 2007, from The New York Times: http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&oref=slogin

Center for Democracy & Technology. (2006, July). *Current Legal Standards for Access To Papers, Records, and Communications: What Information Can the Government Get About You, and How Can They Get It?* Retrieved November 10, 2007, from EDUCAUSE.edu: <http://edUCAUSE.edu/ir/library/pdf/EDU06260C.pdf>

Clinton, W. J., & Gore, J. A. (1997, July 1). *A Framework For Global Electronic Commerce*. Retrieved November 18, 2007, from World Wide Web Consortium: <http://www.w3.org/TR/NOTE-framework-970706.html>

CNNMoney.com. (2007, May 14). *Total Online Sales Expected to Grow 19% to \$174.5B in 2007*. Retrieved November 10, 2007, from CNNMoney.com: http://money.cnn.com/2007/05/14/news/economy/online_retailing/

Katz vs. United States, 389 U.S. 347 (The Supreme Court December 18, 1967).

Kerstein, P. (2005, July 19). *How Can We Stop Phishing and Pharming Scams?* Retrieved November 18, 2007, from CSOnline: <http://www.csonline.com/talkback/071905.html>

LeClaire, J. (2006, September 11). *'Second Life' Gaming Site Suffers Security Breach*. Retrieved November 18, 2007, from TechNewsWorld: <http://www.technewsworld.com/story/52934.html>

Platform for Privacy Preferences (P3P) Project. (n.d.). Retrieved November 18, 2007, from The W3C Consortium: <http://www.w3.org/P3P/>

Rosenbush, S. (2005, July 19). *News Corp.'s Place in MySpace*. Retrieved November 10, 2007, from BusinessWeek.com:

http://www.businessweek.com/technology/content/jul2005/tc20050719_5427_tc119.htm

Schmidt, T. S. (2006, September 6). *Inside the Backlash Against Facebook*. Retrieved November 18, 2007, from TIME.com: <http://www.time.com/time/nation/article/0,8599,1532225,00.html>

Second Life Economics Statistics Page. (2007, November 17). Retrieved November 17, 2007, from SecondLife Web site: http://secondlife.com/whatis/economy_stats.php

Soltren, H. J. (2005). *Facebook: Threats to Privacy*. Cambridge, MA: MIT.

The Gramm-Leach-Bliley Act. (2005, January 21). Retrieved November 18, 2007, from Electronic Privacy Information Center: <http://www.epic.org/privacy/glba/>